ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-20

The Brenda Strafford Foundation Ltd.

August 26, 2013

(Case File #P2282)

I. Introduction

[1] Under s. 34.1 of the *Personal Information Protection Act* (PIPA), an organization having personal information under its control must, without unreasonable delay, notify me of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

[2] On March 5, 2013, the Brenda Strafford Foundation Ltd. (Organization) provided notice of an incident involving the unauthorized disclosure of personal information. For the reasons that follow, I have decided that there is a real risk of significant harm to individuals as a result of the incident. I require the Organization to notify the individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[3] Section 37.1 of PIPA authorizes me to require an organization to notify individuals to whom there is a real risk of significant harm as a result of an incident. It states:

> 37.1(1) Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure
>
> (a) in a form and manner prescribed by the regulations, and

(b) within a time period determined by the Commissioner.

(2) If the Commissioner requires an organization to notify individuals under subsection (1), the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate in addition to the requirements under subsection (1).

(3) The Commissioner must establish an expedited process for determining whether to require an organization to notify individuals under subsection (1) in circumstances where the real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure is obvious and immediate.

(4) The Commissioner may require an organization to provide any additional information that the Commissioner considers necessary to determine whether to require the organization

(a) to notify individuals under subsection (1), or

(b) to satisfy terms and conditions under subsection (2).

(5) An organization must comply with a requirement

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), or

(c) to satisfy terms and conditions under subsection (2).

(6) The Commissioner has exclusive jurisdiction to require an organization

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), and

(c) to satisfy terms and conditions under subsection (2).

(7) Nothing in this section is to be construed so as to restrict an organization's ability to notify individuals on its own initiative of the loss of or unauthorized access to or disclosure of personal information.

[4] PIPA applies to organizations, defined in section 1(1)(i) of PIPA as follows:

1(1) (i) "organization" includes

(i) a corporation,

(ii) an unincorporated association,

(iii) a trade union as defined in the *Labour Relations Code*,

(iv) a partnership as defined in the *Partnership Act*, and

(v) an individual acting in a commercial capacity,

but does not include an individual acting in a personal or domestic capacity;

[5] I considered whether or not PIPA applies to this Organization. Pursuant to section 56(3), PIPA only applies to "non-profit organizations" in respect of personal information that is collected, used or disclosed in connection with a commercial activity. In this case, the Organization is registered in Alberta as a corporation.[1] It is not a "non-profit organization" as defined in section 56(1)(b)(i) of PIPA. I have jurisdiction in this matter because the Organization is an "organization" as defined in section 1(1)(i) of PIPA.

[6] The Organization reported the incident involved the following information:

- name,
- address,
- social insurance number (SIN),
- salary earned in the past year.

[7] This information qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

III. Background

[8] On March 12, 2013, my Office requested the Organization provide additional information. The additional information was provided by the Organization between March 12, and May 13, 2013.

[9] The circumstances of the incident as reported to me by the Organization are as follows:

- On February 20, 2013, the Organization prepared and mailed T4 slips for its employees.
- On February 28, 2013, an employee contacted the Organization to report receiving two T4 slips instead of one. The second T4 slip was for another individual.

[1] Alberta Corporate Registry System – The Brenda Strafford Foundation Ltd., Corporate Access Number: 200365088

- The incident was the result of human error. Two T4 slips instead of one were accidentally inserted into 150 envelopes.
- The result was 150 employees (the Recipients) received their own and another employee's T4 slip.
- The Organization obtained undertakings from 121 Recipients that they did not copy, and would not use or disclose the information provided to them in error. The Organization was unable to reach 29 Recipients.
- The Organization notified all employees affected by the incident in a letter dated March 1, 2013.

IV. Is there a real risk of significant harm to individuals as a result of the incident?

[10] In considering whether to require the Organization to notify the affected individuals, I am mindful of PIPA's purpose, legislative principles, and the relevant circumstances surrounding the reported incident.

[11] Pursuant to section 37.1 of PIPA, I have the power to require the Organization to "notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure." In determining whether or not to require the Organization to notify the affected individuals, I must consider if there is a "real risk of significant harm" to the affected individuals as a result of the incident.

[12] In order for me to require that the Organization notify the affected individuals, there must be some harm – some damage or detriment or injury – that could be caused to those affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.

[13] The Organization reported the personal information involved in this incident is highly sensitive. It indicated that identity theft and fraud could occur as a result of the unauthorized disclosure of the personal information of the affected individuals. The Organization believes the harm may be significant due to the sensitivity of the information involved.

[14] In my view, the personal information is highly sensitive. It includes the names, addresses, SINs, and yearly salaries of the affected individuals. The types of harm that could result from unauthorized access to the personal information in this instance are identity theft or fraud. In my view, these are significant harms.

[15] In order for me to require the Organization to notify the affected individuals, there must also be a "real risk" of significant harm to the affected individuals as a result of the incident. This standard does not require that significant harm will certainly result from the incident, but the likelihood that it will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.

[16] In deciding whether there is a real risk of significant harm to the affected individuals as a result of this incident, I considered the decisions reached in P2011-ND-009, P2011-ND-015, P2012-ND-06, and P2012-ND-05. In each of these decisions, the personal information at issue and cause of the breach were the same or similar to this incident and the Commissioner determined there was a real risk of significant harm existed to the affected individuals.

[17] In this case, the Organization was able to obtain undertakings from 121 of the 150 individuals who received personal information of others in error that they would not use or disclose the information. In my view, there is no real risk of significant harm to these 121 individuals. However, the Organization was unable to obtain a similar undertaking from 29 of the individuals who received personal information in error.

[18] Based on the above and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the 29 affected individuals as a result of this incident. Factors that contributed significantly to my decision are: the personal information involved is highly sensitive, and the Organization was not able to obtain an undertaking from 29 of the individuals who received information in error.

V. Decision

[19] I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

[20] I understand that the Organization has notified the affected individuals in accordance with the Regulation in a letter sent on March 1, 2013. Therefore, I will not require the Organization to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner